## REMARKS

Claims 1 – 104 are pending in the application.

## REJECTIONS UNDER 35 U.S.C. §102

The Examiner has rejected claims 1-104 under 35 U.S.C. §102(b) as being unpatentable over Hill et al. (U.S. Patent No. 6,088,804), herein referred to as Hill.

Regarding independent method claims 1, 13, 21 and 95, the Examiner maintains that Hill discloses "[a] method for detecting malicious code in an information handling system, comprising: executing malicious code detection code (MCDC) on the information handling system, the MCDC including detection routines for gathering information about executable code under investigation, the detection routines including at least one of the following: (a) examining the code or program and (b) searching for information in the information handling system about the code or program, the detection routines including valid program detection routines and malicious code detection routines...", as in claim 13, and cites thereby col. 4, lines 5-61 in Hill. Applicant respectfully disagrees. In contrast, Hill recites that:

> Dynamic network security system 20 includes a plurality of security agents 36 each of which is associated with one or more nodes 24. Security agents 36 are configured to concurrently detect occurrences of security events (discussed below) on associated computer nodes 24. Security agents 36 are software programs located at nodes 24 and area servers 30 that identify security events as they appear at the nodal level. Security events may include port scans, malicious software, penetration attempts, and others that are identified through either a specific code signature or through actions or attempts at actions.
>
> (*See* Hill, col. 4, lines 30-40)

However, Hill does not appear to teach or suggest "...applying the detection routines to executable code under investigation, the detection routines associating weights to respective code under investigation in response to detections of a valid program or malicious code as a function of the detection routines; and determining whether code under investigation is a valid program or malicious code as a function of the weights

associated by the detection routines..." as in claim 1. Further, Hill does not appear to teach or suggest "...the detection routines including valid program routines and malicious code detection routines", as in claim 13. Further, Hill does not appear to teach or suggest "assigning weights as a function of the examined characteristics and behaviors, the assigned weights indicative of a valid program or malicious code as a function of the detection routines; and determining whether executable code under investigation is malicious code as a function of the weights assigned by the detection routines", as in claim 21.

The Examiner further maintains that Hill discloses applying the detection routines to the executable code under investigation, the detection routines associating weights to respective code under investigation in response to detections of a valid program or malicious code as a function of at least one of the detection routines, and determining whether code under investigation is a valid program or malicious code as a function of the weights associated by the detection routines, wherein determining whether the code under investigation is a valid program or malicious code includes scoring an execution of the detection routines as a function of the weights, and wherein scoring includes configuring a scoring algorithm to identify code under investigation as malicious code in response to at least one of a valid score and a malicious code score. Applicant respectfully disagrees and submits that Hill states:

> In addition to security event types 56 and percentage of security events 50 per event type in column 58, training signatures 53 include location identifiers 60. Location identifiers 60 identify the nodes 24 in network 22 where security events may take place. Location identifiers 60 are important for ascertaining an attack severity 61 for each of simulated attacks 52. Attack severity 61 is a level of security breach that one of simulated attacks 52 could cause computer network 22. The greater attack severity 61, the more damaging the security breach would be.
>
> (*See* Hill, col. 5, lines 65 to col. 6, line 8, emphasis added.)

There does not appear to be any teaching or suggestion in Hill of "applying detection routines to the executable code under investigation..." as in claims 1 and 13. Applicant further submits that Hill states that:

> With reference back to FIG. 2, following accessing task 46,

> a task 62 performs first simulated attack 55 (FIG. 3) having a first training signature 54 on computer network 22 (FIG. 1). Those skilled in the art will recognize that first simulated attack 55 is not launched against nodes 24 (FIG. 1) of computer network 22, but rather first simulated attack 55 is input into dynamic network security system 20 (FIG. 1) so that SOM processor 40 (FIG. 1) can receive and process the attack information.
>
> (*See* Hill, col. 6, lines 23-32, emphasis added.)

There does not appear to be any teaching or suggestion in Hill regarding "wherein scoring includes configuring a scoring algorithm to identify code under investigation as malicious code in response to at least one of a valid score and a malicious code score[,]" as in claim 13. Therefore, Applicant respectfully submits that claims 1, 13, 21 and 95 and their associated dependent claims are not anticipated by Hill. Applicant also respectfully submits that computer program claims 41 and 49, and system claims 69 and 77, along with their respective associated dependent claims, are allowable for at least the reasons presented in support of method claims 1, 13 and 21.

Further, Applicant respectfully submits that the Examiner has not indicated which specific teachings in the prior art anticipate the subject matter claims 26-27, 33-40, 54-55, 61, 69, 77, 82-83, 87 and 95-97 under 35. U.S.C. §102.

For a claim to be anticipated under 35 U.S.C. §102, each and every claim limitation must be found within the cited prior art reference and arranged as required by the claim. M.P.E.P. §2131. Since the Examiner has not shown how each limitation in claims 1-104 is found in Hill, Applicant respectfully submits that claims 1-104 are not anticipated by Hill. Removal of the rejection of claims 1-104 under 35. U.S.C. §102 is requested.

**REJECTIONS UNDER 35 U.S.C. §103**

The Examiner has rejected claims 26-27, 54-55 and 82-83 under 35 U.S.C. §103(a) as being unpatentable over Hill in view of Arnold et al. (U.S. Patent No. 5,440,723), herein referred to as Arnold.

Regarding dependent claims 26-27, 54-55 and 82-83, the Examiner asserts that Arnold discloses "wherein the scoring algorithm determines a valid program by a summation of weights of the valid program detection routines being greater than a valid program weight threshold, and a malicious code by a summation of weights of the malicious code detection routine having a summed value greater than a malicious code weight threshold." Applicant respectfully disagrees and submits that neither Arnold, nor the references cited therein, teach or suggest the limitations in these claims.

Applicant respectfully submits that no objective evidence or suggestion of a motivation to combine Hill with Arnold has been presented by the Examiner. The motivation applied by the Examiner for combining thus appears to be gleaned directly from Applicant's disclosure.

As a result of the foregoing Applicant respectfully submits that the Examiner has not established a *prima facie* case of obviousness in rejecting claims 26-27, 54-55 and 82-83. Removal of the rejection of claims 26-27, 54-55 and 82-83 under 35 U.S.C. §103 is requested.

In light of the foregoing amendments and remarks, Applicants submit that all pending claims are now in condition for allowance, and an early notice to that effect is earnestly solicited. If a phone interview would speed allowance of any pending claims, such is requested at the Examiner's convenience.

The Commissioner is authorized to charge any fees which may be required, or credit any overpayment, to Meyertons, Hood, Kivlin, Kowert & Goetzel, P.C. Deposit Account No. 501505\6002-00602.

Respectfully submitted,

B. Noël Kivlin
Reg. No. 33,929
ATTORNEY FOR APPLICANTS

Meyertons, Hood, Kivlin, Kowert & Goetzel, P.C.
P.O. Box 398
Austin, TX 78767-0398
(512) 853-8800
Date: 6-23-06